PATENT
Atty Docket No.: 100200290-1

In The U.S. Patent and Trademark Office

In Re the Application of:

Inventor(s)	Zhichen XU et al.	Confirmation No.	7480
Serial No.:	10/084,499	Examiner: Jeffery L. Williams	
Filed:	February 28, 2002	Group Art Unit:	2137

Title: INCREASING PEER PRIVACY

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF FACSIMILE TO THE USPTO

I hereby certify that this correspondence is being transmitted to the Patent and Trademark Office facsimile number (571) 273-8300 on January 2, 2007. This correspondence contains the following document(s):

1 sheet of Transmittal of Appeal Brief (2 copies).

37 sheets of Appeal Brief – Patents

Respectfully submitted,

MANNAVA & KANG, P.C.

January 2, 2007

Ashok K. Mannava
Reg. No.: 45,301

MANNAVA & KANG, P.C.
8221 Old Courthouse Road
Suite 104
Vienna, VA 22182
(703) 652-3822
(703) 865-5150 (facsimile)

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. __100200290-1__

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL FAX CENTER

JAN 2 - 2007

Inventor(s):   Zhichen XU et. al

Application No.: 10/084,499

Filing Date: Feb. 28, 2002

Title: INCREASING PEER PRIVACY

Confirmation No.: 7480

Examiner: Jeffery Williams

Group Art Unit: 2137

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on __Nov. 2, 2006__.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

         ( ) one month $120.00
         ( ) two months· $450.00
         ( ) three months $1020.00
         ( ) four months $1590.00

     ( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of __$500.00__. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

( ) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit:_____

OR

(X) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number_(571) 273-8300___ on ___Jan. 2, 2007___

Number of pages: 40

Respectfully submitted,

Zhichen XU et. al

By _____
Ashok Mannava

Attorney/Agent for Applicant(s)
Reg. No. 45,301

RECEIVED
CENTRAL FAX CENTER

JAN 2 - 2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Attorney Docket No.: 100200290-1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s)	Zhichen XU et al.	Confirmation No.	7480
Serial No.:	10/084,499	Examiner: Jeffery L. Williams	
Filed:	February 28, 2002	Group Art Unit:	2137
Title:	INCREASING PEER PRIVACY		

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF - PATENTS

Sir:

This is an Appeal Brief in connection with the decisions of the Examiner in a final Office

Action mailed August 2, 2006 and in connection with the Notice of Appeal mailed November 2,

2006. It is respectfully submitted that the present application has been more than twice rejected.

Each of the topics required in an Appeal Brief and a Table of Contents are presented herewith

and labeled appropriately.

PATENT   Atty Docket No.: 100200290-1
                                          App. Ser. No.: 10/084,499

TABLE OF CONTENTS

2

PATENT

<div align="right">

Atty Dockcl No.: 100200290-1
App. Ser. No.: 10/084,499

</div>

(1)   **Real Party In Interest**

The real party in interest is Hewlett-Packard Development Company, L.P.

(2)   **Related Appeals And Interferences**

There are no other appeals or interferences related to this case.

(3)   **Status Of Claims**

Claims 1, 3-12, 14-25, 27-30 and 42-44 are pending of which claims 1, 12, 21 and 42 are

independent. Claims 2, 13, 26 and 31-41 were previously canceled, and claims 43-44 were

previously added. All pending claims 1, 3-12, 14-25, 27-30 and 42-44 are hereby appealed.

(4)   **Status of Amendments**

No amendment was filed subsequent to the final Office Action dated August 2, 2006.

(5)   **Summary Of Claimed Subject Matter**

A conventional system of peers (or network nodes) interconnected via a network, such as

in the Internet, provides a relatively convenient means of exchanging information between the

peers. However, conventional network systems may be vulnerable to malicious users. For

example, malicious users may determine the types of information stored at specific peers by

monitoring the network traffic on the network. This may be problematic if one or more of the

3

PATENT   Atty Docket No.: 100200290-1
                                              App. Ser. No.: 10/084,499

peers are a source of sensitive information.

According to embodiments described in the Applicants' specifications, systems and

methods are described for anonymizing network paths and peer identities to increase peer

privacy and to prevent malicious users from gaining access to information by monitoring

network traffic. In one embodiment, when a peer requests information, an anonymous and

varying network path, which may include randomly selected peers, is initially formed for

transmitting the requested information from a provider to the requestor. For example, a trusted

third party, such as the directory 130 shown in figure 1, receives requests for information. The

trusted third party may include a database storing peer information. The directory 130, acting as

a trusted-third-party (i.e., configured not to reveal identities and/or modify information), searches

the database for the availability of the requested information. If the information is available on a

peer, referred to as the provider peer, the directory 130 forms a network path between the

provider peer and the requestor peer. For example, the directory 130 randomly selects a sub-

group of peers (or other selection criteria known to those skilled in the art may be used) to be in

the path, which includes the requestor peer as the last segment of the path. See page 6, lines 3-

14.

After selecting the peers for the path, the directory 130 transmits a respective set-up

message to each of the peers in the selected sub-group. Each set-up message may comprise a

path index entry, which includes at least an individual predetermined label and an identity of a

next peer according to the path. The path index entry may provide an approach for peers

receiving messages to determine the next hop or segment for a particular received message. See

4

PATENT   Atty Docket No.: 100200290-1
                                              App. Ser. No.: 10/084,499

page 6, lines 15-20.

Each peer in the selected subgroup receiving the set-up message updates a respective

hash table with the received label and identity of the next peer for the information according to

the path. When a retrieval message is being transmitted along the path to the requestor peer,

including the requested information or a reference to the requested information, each peer

receiving the message uses a label in the received message to search its hash table for a matching

label, previously received in the set-up message, to retrieve the identity of the next peer in the

path. See page 6, line 21-page 7, line 6.

In one embodiment, the label is generated using the selected group of peers and a second

selected group of index peers. The label for a peer in the selected subgroup of peers forming the

path is generated using a corresponding index peer of the selected group of index peers

according to equation 1 on page 20. In particular, the label for the current peer is generated by

encrypting the label of the previous peer with the public key of the current index peer.

Accordingly, to generate a label for the peer next to the current peer, the peer privacy module

330 of the directory 130 encrypts the current label with a public key of the next index peer. This

information is transmitted in the set-up message to the current peer, so when the current peer

receives the retrieval message it uses the current label with a public key of the next index peer to

transmit the retrieval message to the next peer in the path. See page 20, line 17-page 21, line 7.

Furthermore, in one embodiment where the index peers are used and during the set-up

stage when the directory 130 is transmitting the set-up messages to the sub-group of selected

peers, an encryption key for a corresponding index peer is used to encrypt a label. In particular,

5

PATENT

as described with respect to figure 7A, a peer may receive a set-up message with a label matching a previously stored label. The peer generates the next state of the label for transmission to the next peer in the path. The next state of the received label may be generated by encrypting the received label with the public key of the respective index peer of the next peer. See page 28, lines 1-3.

Support for the features recited in independent claims 1, 12, 21 and 42 is as follows:

1. A method for increasing peer privacy, comprising:

forming a path from a provider to a requestor by selecting a plurality of peers in response to receiving a request for information; See page 6, lines 3-14; page 18, line 9-page 21, line 7; Figures 4A-B, steps 405-460.

updating a table on each peer of said plurality of peers with a respective path index entry for said information; See page 6, line 21-page 7, line 6; Figure 7A, steps 705-730; page 27, line 7-page 28, line 10.

transmitting a message to said requestor through said plurality of peers, said message comprising said information and a path index for said information from said provider; See page 7, line 7-page 8, line 8; page 24, line 18-page 25, line 22; Figure 6A, steps 605-625, 640 and 645.

determining a next peer according to said path for said information by searching said table of each peer of said plurality of peers with said path index as an index into said table; See page 7, line 22-page 8, line 8; page 25, lines 18-21; Figure 6A, step 640.

6

retrieving an identity of said next peer according to said path for said information and a respective index peer of said next peer; See page 20, line 17-page 21, line 7; Figure 6A, steps 605-625, 640 and 645.

encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index; See Figures 6A-B, steps 645 and 650; page 26, lines 4-6.

transmitting a new message with said information and said next state of said path index as said path index to said next peer. See Figure 6B, step 660; page 26, lines 8-9.

12.   A method of transmitting information, comprising:

updating a respective table of each peer of a plurality of peers with a respective path index entry in response to receiving a path formation message containing said respective path index entry; See page 6, line 21-page 7, line 6; Figure 7A, steps 705-730; page 27, line 7-page 28, line 10.

receiving a message comprising said information and a path index; See Figure 6A, step 610; page 25, lines 4-7; Figure 5, step 510.

forwarding said information to a next peer in response to a determination of said next peer from said table with said path index as a search index into said table; See Figure 6B, steps 650-660; page 26, lines 1-9; Figure 5, step 540.

7

PATENT

forming a next state of said path index by encrypting said path index with a public

key of a respective index peer of said next peer; See Figure 6B, steps 650-660; page 26, lines 1-

9.

forming a new message with said information and said next state of said path

index as said path index; and See Figure 6B, steps 650-660; page 26, lines 1-9.

transmitting said new message to said next peer. See Figure 6B, steps 650-660;

page 26, lines 1-9.

21. (Previously Presented) A method of increasing peer privacy, comprising:

selecting a path for information from a provider to a requestor through a plurality

of peers in response to a received request for said information; See page 6, lines 3-14; page 18,

line 9-page 21, line 7; Figures 4A-B, steps 405-460.

receiving a respective set-up message at each peer of said plurality of peers,

wherein said respective set-up message comprises a predetermined label and an identity of a next

peer for said information according to said path; See page 6, line 21-page 7, line 6; page 13, lines

4-21; Figure 7A, steps 705-730; page 27, line 7-page 28, line 10.

generating an encryption key; See page 17, lines 12-17; Figure 4B, step 465; page

21, lines 10-13.

encrypting said encryption key with a public key of said requestor; See page 17,

lines 12-17; Figure 4B, step 470; page 21, lines 14-16.

8

PATENT   Atty Docket No.: 100200290-1
                                                    App. Ser. No.: 10/084,499

 encrypting said encryption key with a public key of said provider; and See page

17, lines 12-17; Figure 4B, step 470; page 21, lines 14-16.

 encrypting a transaction identifier, a reference for said information, and a first

next peer according to said path with said encryption key. See page 17, lines 12-17; page 20,

lines 5-8 and lines 15-16; Figure 4B, steps 445 and 475; page 21, lines 17-20;

 42. (Previously Presented) A method of increasing peer privacy, comprising:

 forming a path for information from a provider to a requestor through a plurality

of peers in response to a received request for said information; See page 6, lines 3-14; page 18,

line 9-page 21, line 7; Figures 4A-B, steps 405-460.

 transmitting to each peer of said plurality of peers a respective set-up message

comprising of a predetermined label and an identity of a next peer for said information; See page

6, line 15-20; page 17, lines 8-11; Figure 4B, step 455; page 21, lines 5-7.

 if a label stored at an intermediate peer of the plurality of peers does not match the

predetermined label in the set-up message, the intermediate peer stores the predetermined label

and the corresponding identity of the next peer; Figure 7A, steps 710-730; page 27, line 11-18;

see page 13, lines 14-21.

 if a label stored at the intermediate peer matches the predetermined label, the

intermediate peer retrieves a previously stored message and generates a next state of the

predetermined label for the setup message; and Figure 7A, steps 735-740; page 27, line 19-page

28, line 3; see page 13, lines 14-21.

9

PATENT   Atty Docket No.: 100200290-1
                                                App. Ser. No.: 10/084,499

        transferring said information over said path in a message by determining a next

peer according to said path by matching a message label included in said message to said

predetermined label. See Figure 6B, steps 650-660; page 26, lines 1-9; page 22, lines 15-18.

(6)   Grounds of Rejection to be Reviewed on Appeal

        A.   Whether the specification should have been objected to for failing to provide

proper antecedent basis for features in claim 42 and for failing to provide support for the features

in claim 44.

        B.   Whether claims 42-44 should have been rejected under 112 first paragraph for

failing to comply with the written description requirement because the subject matter in claims

42 and 44 was not described in the specification in such a way as to reasonably convey to one

skilled in the relevant art that the inventors, at the time the application was filed, had possession

of the claimed invention.

        C.   Whether claims 1, 8-12, 20-25, 27-30 and 42-44 should have been rejected under

35 U.S.C. §102(b) as being anticipated by Goldschlag et al., "Hiding Routing Information";

hereinafter referred to as Goldschlag.

        D.   Whether claims 3-7 and 14-19 should have been rejected under 35 U.S.C. §103(a)

as being unpatentable over Goldschlag in view of Clark et al.,"Freenet: A Distributed

Anonymous Information Storage and Retrieval System", hereinafter referred to as Clarke.

                                        10

PATENT

<div align="right">Atty Docket No.: 100200290-1
App. Ser. No.: 10/084,499</div>

(7)   **Arguments**

A.   The objection to the specification for failing to provide proper antecedent basis for features in claim 42 and for failing to provide support for the features in claim 44 is improper; and

B.   The rejection of claims 42-44 under 112 first paragraph for failing to comply with the written description requirement is improper.

On page 2 of the office action, the specification was objected to for the following reasons:

> Claim 42 recites the limitations "if a label stored at an intermediate peer of the plurality of peers does not match the predetermined label in the set-up message, the intermediate peer stores the predetermined label and the corresponding identity of the next peer" [emphasis added]. The specification does not provide antecedent basis for storing the predetermined label upon condition that a label does not match.

> Claim 44 recites the limitation, wherein the stored message comprises: an encryption key encrypted with the public key of the requestor". This limitation is not supported in the specification.

Regarding the objection with respect to claim 42, the specification clearly discloses that the peer privacy module 220 at an intermediate peer may be configured to search the hash table 225 for an existing entry matching the received current label. If the existing entry is not present, the hash table 225 may be updated with the label and the corresponding identity for the next peer according to the path. Otherwise, if there is an existing entry, the peer privacy module 220 may

<div align="center">11</div>

PATENT

be configured determine the next peer according to the path and to retrieve a previously stored message. The peer privacy module 220 may also be configured to reformat the previously stored message with the received label encrypted with a public key of the next peer as the label for the message for transmission to the next peer. Figure 7A, steps 710-730; page 27, line 11-18; see page 13, lines 14-21.

Based at least on this disclosure and the disclosure with respect to figure 7A, the specification clearly discloses storing the predetermined label upon condition that a label does not match. As described above, the hash table 225, which may be stored in the peer (See figure 2 and page 11, lines 15-18), is updated with the received current label if there is no match.

Regarding the objection with respect to claim 44, the specification clearly discloses an encryption key encrypted with the public key of the requestor. For example, the directory 130 may include a peer privacy module 330 transmitting a retrieval message with an encryption key encrypted with the public key of the requestor. See page 17, lines 12-17. An intermediate peer may receive and store the retrieval message with the encryption key encrypted with the public key of the requestor. See page 12, lines 13-22. Also, step 635 in figure 6A clearly states storing the received message. This is the retrieval message with the encrypted information. See page 25, line 6-16.

The rejection of claim 42-44 under 112 first paragraph for lack of written description was based on the objection to the specification, according to page 3 of the office action. As described above, the specification clearly discloses the features of claims 42 and 44 in the application as originally filed, and thus the specification clearly describes in such a way as to reasonably

12

PATENT   Atty Docket No.: 100200290-1
                                                    App. Ser. No.: 10/084,499

convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. Thus, the objections to the specification and the rejection of claim 42-44 under 112 first paragraph for lack of written description are believed to be improper.

C.   The rejection of claims 1, 8-12, 20-25, 27-30 and 42-44 under 35 U.S.C. §102(b) as being anticipated by Goldschlag is improper

The test for determining if a reference anticipates a claim, for purposes of a rejection under 35 U.S.C. § 102, is whether the reference discloses all the elements of the claimed combination, or the mechanical equivalents thereof functioning in substantially the same way to produce substantially the same results. As noted by the Court of Appeals for the Federal Circuit in *Lindemann Maschinenfabrick GmbH v. American Hoist and Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984), in evaluating the sufficiency of an anticipation rejection under 35 U.S.C. § 102, the Court stated:

> Anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim.

Therefore, if the cited reference does not disclose each and every element of the claimed invention, then the cited reference fails to anticipate the claimed invention and, thus, the claimed invention is distinguishable over the cited reference.

13

PATENT

Atty Docket No.: 100200290-1
App. Ser. No.: 10/084,499

The Examiner clearly failed to apply the aforementioned test for anticipation under 35 U.S.C. § 102 because Goldschlag fails to teach all the features of independent claims 1, 12, 21 and 42.

Independent claim 1

Claim 1 recites:

> retrieving an identity of said next peer according to said path for said information and a respective index peer of said next peer;
> encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index; and
> transmitting a new message with said information and said next state of said path index as said path index to said next peer.

Goldschlag fails to teach an index peer of a next peer; retrieving an identity of a next peer according to said path for said information and a respective index peer of said next peer; and encrypting the path index with public key of the index peer of the next peer. There are no index peers in Goldschlag, and accordingly, Goldschlag fails to teach a respective index peer and encrypting the path index with public key of the index peer of the next peer.

The rejection of claim 1 on page 4, lines 16-20 and page 16, lines 8-12 states that encrypting the path index with a public key of the index peer of the next peer is taught on page 5, page 11 and figure 2 of Goldschlag. Accordingly, the description with respect to page 5, page 11 and figure 2 of Goldschlag is discussed below.

14

PATENT   Atty Docket No.: 100200290-1
                                            App. Ser. No.: 10/084,499

With respect to page 5 and figure 2 of Goldschlag, Goldschlag discloses encrypting an

onion with a public key of a next peer but fails to teach encrypting the onion with a public key of

an index peer of the next peer. In particular, Goldschlag discloses a forward onion in figure 2.

The onion is a data structure composed of layer upon layer of encryption wrapped around a

payload. See pages 4-5. The basic structure of the onion is based on the route to the responder

that is chosen by the initiator's proxy.

Goldschlag discloses on page 5 that the data structure of an onion received at a node Px

looks like this:

   {*exp time, next hop, Ff, Kf, Fb, Kb*, payload}PKx

Here PK is a public encryption key for routing node P, who is assumed to have the

corresponding decryption key. The onion is encrypted with the public encryption key, PKx, of

the next routing node in the predetermined route determined by the initiator's proxy. See last

paragraph of page 4 and page 5. An index peer for a next node is not disclosed in Goldschlag

and using a public key of an index peer for a next node is not disclosed in Goldschlag.

With regard to page 11 of Goldschlag and other related passages, Goldschlag discloses

that the two function key pairs, i.e., *Ff, Kf, Fb, Kb*, specify the cryptographic operations and keys

to be applied to data that will be sent along the virtual circuit. See page 5. Use of the functions

keys for encrypting data is further described in section 4 "Implementation" in Goldschlag. See

page 9. After using the "create" command to establish virtual circuit, the "data" command is

used to pass a stream of data from the initiator to the responder. The initiator node breaks the

data stream into payload sized chunks, and repeatedly pre-crypts each chunk of the data stream

15

PATENT   Atty Docket No.: 100200290-1
                                                    App. Ser. No.: 10/084,499

using the inverse of the cryptographic operations specified in the onion, innermost first. At a

node receiving the onion, the function/key pairs that are applied, and the virtual circuit identifier

of the connection to the next node are obtained from a table. The cryptographic function key

pair associated with the circuit (for the appropriate direction) and the virtual circuit identifier of

the connection to the next node is obtained. It then peels off a layer of cryptography and

forwards the peeled payload to the next node.

Thus, Goldschlag discloses encrypting payload data of the data stream with the function

key pairs. However, the virtual circuit identifier in Goldschlag is not encrypted with the function

key pairs or a public key of an index peer of a next peer. Accordingly, the rejection of claims 1

and 3-11 is believed to be improper and these claims are believed to be allowable. Also, claim

11 is directed to an index entry including respective index peers, which is not taught by

Goldschlag.

On page 16, lines 8-12 of the Office Action, the Examiner states:

The examiner respectfully notes that Goldschlag discloses utilizing
identity information to retrieve the identity of the next peer and encrypting the
message with the public key associated with the identity information. Thus
Goldschlag teaches *an index peer of a next peer* and *encrypting the path
index with public key of the index peer of the next peer.*

16

PATENT   Atty Docket No.: 100200290-1
                                                App. Ser. No.: 10/084,499

As described above and as clearly stated on page 5 of Goldschlag, the only public key

disclosed in Goldschlag is PK, which is a public encryption key for routing node P, who is

assumed to have the corresponding decryption key. That is, the onion is encrypted with the

public encryption key, PKx, of the next routing node in the predetermined route. The Examiner

appears to allege that Goldschlag discloses a public key associated with the identity information

for a next node, and thus Goldschlag discloses a public key of an index peer for a next node.

Firstly, Goldshlag fails to disclose a public key associated with the identity information for a

next node. Instead, Goldschlag discloses a public key for the actual next node and not the public

key for an index node of the next node. Secondly, assuming arguendo that Goldschlag discloses

a public key associated with the identity information for a next node, Goldschlag fails to teach

identity information that is an index peer for a next node. The Examiner appears to completely

disregard the specific recitation in the claim of "a public key of said respective index peer of said

next peer." Goldschlag fails to teach index peers for the routing nodes, and encrypting messages

with a public key of a respective index peer for a routing node.

Independent claim 12

Independent claim 12 recites, "forming a next state of said path index by encrypting said

path index with a public key of a respective index peer of said next peer." For the reasons stated

above with respect to claim 1, Goldschlag fails to teach encrypting said path index with a public

17

PATENT

Atty Docket No.: 100200290-1
App. Ser. No.: 10/084,499

key of a respective index peer of said next peer. Accordingly, the rejection of claims 12 and 14-

20 is believed to be improper and these claims are believed to be allowable.

Independent claim 21

Independent claim 21 recites, "selecting a path for information from a provider to a

requestor through a plurality of peers in response to a received request for said information."

Goldschlag discloses on page 4, beginning of section 3:

> To begin a session between an initiator and a responder, the initiator's
> proxy identifies a series of routing nodes forming a route through the network and
> constructs an onion which encapsulates that route. Figure 2 illustrates an onion
> constructed by the initiator's Proxy/Routing Node W for an anonymous route to
> the responder's Proxy/Routing Node Z through intermediate routing nodes X and
> Y. The initiator's proxy then sends the onion along that route to establish a virtual
> circuit between himself and the responder's proxy.

Thus, Goldschlag discloses identifies a series of routing nodes between an initiator and a

requestor forming a route through the network, and Goldschlag discloses constructing an onion

which encapsulates that route.

Claim 21 also recites:

> generating an encryption key;
> encrypting said encryption key with a public key of said requestor;

18

PATENT

>   encrypting said encryption key with a public key of said provider;
> and
>   encrypting a transaction identifier, a reference for said information,
> and a first next peer according to said path with said encryption key.

As described above and as shown in figure 2, Goldschlag discloses that the two function key pairs, *i.e.*, *Ff, Kf, Fb, Kb*, specify the cryptographic operations and keys to be applied to data that will be sent along the virtual circuit. However, Goldschlag fails to teach encrypting *Ff, Kf, Fb, Kb* with the encryption key of the initiator. Instead, the outer most layer of the onion would include *Ff, Kf, Fb, Kb* encrypted with the public key, *Pk*, of the routing node next to the initiator. See last paragraph of page 4. Thus, the onion does not include encrypting *Ff, Kf, Fb, Kb* with the encryption key of the initiator. Hence, Goldschlag fails to teach encrypting said encryption key with a public key of said provider.

The rejection of claim 21 alleges that the claimed encrypting a transaction identifier is taught by Goldschlag encrypting an expiration time for the onion, exp_time, in the onion. Goldschlag discloses that if a node receives an onion with an expired expiration time, the onion is ignored. See first full paragraph on page 5. However, the expiration time is not an identifier of a transaction. Instead, the expiration time is used to determine whether to ignore an onion, but is not used to identify the onion and is not used to identify a transaction for the onion. Because Goldschlag fails to teach using the expiration time as an identifier, Goldschlag fails to teach encrypting a transaction identifier.

19

PATENT

The rejection of claim 21 also alleges that the claimed encrypting a reference for said information is taught by Goldschlag encrypting a payload in the onion. However, Goldschlag fails to teach the payload comprises a reference to requested information. Simply because Goldschlag discloses a payload, does not necessarily require that the payload include a reference to requested information. Accordingly, Goldschlag fails to teach encrypting a reference to requested information. Accordingly, the rejection of claims 21-25 and 27-30 is believed to be improper and these claims are believed to be allowable.

Independent claim 42

Claim 42 recites:

> if a label stored at an intermediate peer of the plurality of peers does not match the predetermined label in the set-up message, the intermediate peer stores the predetermined label and the corresponding identity of the next peer;
> if a label stored at the intermediate peer matches the predetermined label, the intermediate peer retrieves a previously stored message and generates a next state of the predetermined label for the setup message.

Goldschlag discloses a create message in section 4 "Implementation" used to create the virtual circuit. However, Goldschlag fails to teach retrieving a previously stored message if there is a match between a received label in a set-up message and a stored label and generating a next state of the predetermined label for the setup message if there is a match. Also, Goldschlag fails to teach, if there is no match, storing the predetermined label and the corresponding identity of

20

PATENT   Atty Docket No.: 100200290-1
                                              App. Ser. No.: 10/084,499

the next peer. There is no comparison performed in Goldschlag to determine whether there is a

match or is not a match between a label in a received set-up message and a stored label.

Accordingly, these features are not taught by Goldschlag and the rejection of claims 42-44 is

believed to be improper and these claims are believed to be allowable.   .

Also, dependent claim 43 recites, "encrypting the received predetermined label with a

public key of a respective index peer of the next peer." These features are not taught by

Goldschlag as described above with respect to claim 1, because Goldschlag fails to teach the

claimed index peer and encrypting with a public key of an index peer for a next peer.

D.   The rejection of claims 3-7 and 14-19 under 35 U.S.C. §103(a) as being unpatentable

over Goldschlag in view of Clark is improper

The test for determining if a claim is rendered obvious by one or more references for

purposes of a rejection under 35 U.S.C. § 103 is set forth in MPEP § 706.02(j):

> To establish a *prima facie* case of obviousness, three basic criteria
> must be met. First, there must be some suggestion or motivation,
> either in the references themselves or in the knowledge generally
> available to one of ordinary skill in the art, to modify the reference or
> to combine reference teachings. Second, there must be a reasonable
> expectation of success. Finally, the prior art reference (or references
> when combined) must teach or suggest all the claim limitations. The
> teaching or suggestion to make the claimed combination and the   .
> reasonable expectation of success must both be found in the prior art
> and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20
> USPQ2d 1438 (Fed. Cir. 1991).

21

PATENT   Atty Docket No.: 100200290-1
                                                   App. Ser. No.: 10/084,499

Therefore, if the above-identified criteria are not met, then the cited reference(s) fails to

render obvious the claimed invention and, thus, the claimed invention is distinguishable over the

cited reference(s).

Claims 3-7 and 14-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over

Goldschlag in view of Clark.

Clark discloses a system where each node in a peer-to-peer network maintains its own

data store. Hash tables are used to determine where to send a request. A key and a hops-to-live

value are specified in a request. A node receiving the request determines whether it stores the

requested data. If not, the receiving node looks up the nearest key in its routing table and

forwards the request to the corresponding node. If the data is found at a node receiving the

request, the data is sent back to the requestor. If Clarke is combined with Goldschlag, each node

in the peer-to-peer network would have to know a path between itself and a requestor to provide

the Onion routing of Goldschlag. This is unlikely in a large peer-to-peer network, and

furthermore would waste valuable data storage space. According to an embodiment of the

Applicants' system, a directory 130 shown in figure 1, such as trusted node, determines paths for

requests and transmits a set-up message to all the nodes in the path. In this embodiment, each

node in the system 100 does not need to know of other peers that can form a path between a

provider and a requestor, because the directory 130 stores that information.

Neither Clarke nor Goldschlag discloses a peer similar to the directory 130, and

furthermore, Clarke fails to disclose that each node in the peer-to-peer network would have to

know a path between itself and a requestor. It is highly unlikely that a peer in Clark, especially

22

PATENT   Atty Docket No.: 100200290-1
                                                App. Ser. No.: 10/084,499

in a large peer-to-peer network such as the Internet, would know a complete path between itself

and a requestor to provide the Onion routing of Goldschlag. Typical routing tables may include

destinations to nearest neighbors, but may not include a path between itself and every node in the

network. Furthermore, requiring each peer to store large tables including path information for

every peer is unrealistic and would waste valuable data storage space. Thus, there is

unreasonable expectation of success when combining the onion routing of Goldschlag with

Clarke. Accordingly, a *prima facie* case of obviousness has not been established and the

rejection should be withdrawn because there is an unreasonable expectation of success.

Accordingly, the rejection of claims 3-7 and 14-19 is believed to be improper and these claims

are believed to be allowable.

23

PATENT

<div align="right">Atty Docket No.: 100200290-1
App. Ser. No.: 10/084,499</div>
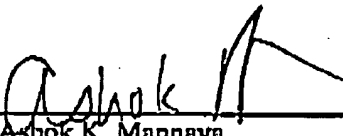
(8)   Conclusion

For at least the reasons given above, the rejection of claims 1, 3-20, and 22-29 is improper. Accordingly, it is respectfully requested that such a rejection by the examiner be reversed and these claims be allowed. Attached below for the Board's convenience is an Appendix of claims 1, 3-20, and 22-29 as currently pending and on appeal.

Please grant any required extensions of time and charge any fees due in connection with this Appeal Brief to deposit account no. 08-2025.

<div align="center">Respectfully submitted,</div>

Dated: January 2, 2007   By

Ashok K. Mannava
Registration No.: 45,301

MANNAVA & KANG, P.C.
8221 Old Courthouse Road
Suite 104
Vienna, VA 22182
(703) 652-3822
(703) 865-5150 (facsimile)

<div align="center">24</div>

PATENT   Atty Docket No.: 100200290-1
                                                  App. Ser. No.: 10/084,499

(9)   **Claim Appendix**

1. A method for increasing peer privacy, comprising:

forming a path from a provider to a requestor by selecting a plurality of peers in response to receiving a request for information;

updating a table on each peer of said plurality of peers with a respective path index entry for said information;

transmitting a message to said requestor through said plurality of peers, said message comprising said information and a path index for said information from said provider;

determining a next peer according to said path for said information by searching said table of each peer of said plurality of peers with said path index as an index into said table;

retrieving an identity of said next peer according to said path for said information and a respective index peer of said next peer;

encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index; and

transmitting a new message with said information and said next state of said path index as said path index to said next peer.

2. (Canceled).

3. The method according to claim 1, further comprising:

25

PATENT   Atty Docket No.: 100200290-1
                                                    App. Ser. No.: 10/084,499

     receiving said request for information at a directory;

     determining an availability of said information; and

     notifying said requestor of a determination of non-availability.

4. The method according to claim 1, further comprising:

     receiving said request for information at a directory;

     determining an availability of said information; and

     generating an encryption key in response to a determination of said availability.

5. The method according to claim 4, further comprising:

     determining a first next peer from said provider and a respective index peer for said first next peer according to said path; and

     encrypting a reference to said information, said first next peer, and said respective index peer of said first next peer with said encryption key.

6. The method according to claim 5, wherein said encryption key is generated according to a DES encryption algorithm.

7. The method according to claim 5, further comprising:

     encrypting said encryption key with a public key of said requestor;

     encrypting said encryption key with a public key of said provider;

26

PATENT

forming a provider message, wherein said provider message comprises:

said encryption key encrypted with said public key of said requestor;

said encryption key encrypted with said public key of said provider;

said encrypted reference; and

said encrypted first next peer and said respective first index peer; and

transmitting said message to said provider.

8. The method according to claim 1, further comprising:

forming a respective path message to each peer of said plurality of peers, said respective path message comprising said respective path index entry.

9. The method according to claim 8, wherein said respective path index entry comprises an identity of a next peer according to said path, a respective index peer for said next peer, and an index entry.

10. The method according to claim 8, wherein said identity of next peer according to said path and said respective index peer for said next peer are encrypted with a public key of a peer receiving said respective path message.

11. The method according to claim 8, wherein said index entry is formed according to $\{ public_{b_i}, (...public_{b_n} (public_{b_n} (n))..) \}$, where b_j represents said respective index peer.

27

PATENT   Atty Docket No.: 100200290-1
                                                    App. Scr. No.: 10/084,499

12. A method of transmitting information, comprising:

updating a respective table of each peer of a plurality of peers with a respective

path index entry in response to receiving a path formation message containing said respective

path index entry;

receiving a message comprising said information and a path index;

forwarding said information to a next peer in response to a determination of said

next peer from said table with said path index as a search index into said table;

forming a next state of said path index by encrypting said path index with a public

key of a respective index peer of said next peer;

forming a new message with said information and said next state of said path

index us said path index; and

transmitting said new message to said next peer.

13. (Canceled).

14. The method according to claim 12, further comprising:

determining an availability of information in response to receiving a request for

information from a requestor; and

notifying said requestor of a determination of non-availability.

28

15. The method according to claim 12, further comprising:

    determining an availability of information in response to receiving a request for information from a requestor; and

    forming a path through a plurality of peers with a provider as a beginning of said path to said requestor in response to a determination of availability.

16. The method according to claim 15, further comprising:

    generating an encryption key;

    determining a first next peer from said provider according to said path and a respective index peer to said first next peer;

    encrypting a reference to said information, said first next peer and said respective index peer with said encryption key; and

    transmitting a retrieval message to said provider, said message comprises:

        said encrypted reference;

        said encrypted first next peer;

        said encrypted respective index peer of said first next peer;

        a value of a message counter for said information;

        said encryption key encrypted with a public key of said provider; and

        said encryption key encrypted with a public key of said requestor.

29

PATENT

17. The method according to claim 15, wherein said generation of said encryption key utilizes a DES encryption algorithm.

18. The method according to claim 15, further comprising:

receiving said second message at said provider;

applying a complementary key to said public key of said provider to said obtain said encryption key; and

applying said encryption key to said encrypted reference to retrieve said reference.

19. The method according to claim 18, further comprising:

retrieving said information based on said decrypted reference;

encrypting said information with said encryption key;

forming said message, wherein said message comprises:

said encrypted information;

encryption key encrypted with a public key of said requestor; and

said path index formed by encrypting said value of message counter with a public key of said respective index peer of said first next peer; and

transmitting said message to said first next peer according to said path.

20. The method according to claim 12, further comprising:

30

PATENT   Atty Docket No.: 100200290-1
                                                               App. Ser. No.: 10/084,499

receiving said message at said requestor;

applying a complementary key to said public key of said requestor to said encryption key encrypted with said public key of said requestor to obtain said encryption key;

applying said encryption key to said encrypted reference to retrieve said information.

21. A method of increasing peer privacy, comprising:

selecting a path for information from a provider to a requestor through a plurality of peers in response to a received request for said information;

receiving a respective set-up message at each peer of said plurality of peers, wherein said respective set-up message comprises a predetermined label and an identity of a next peer for said information according to said path;

generating an encryption key;

encrypting said encryption key with a public key of said requestor;

encrypting said encryption key with a public key of said provider; and

encrypting a transaction identifier, a reference for said information, and a first next peer according to said path with said encryption key.

22. The method according to claim 21, further comprising:

updating a table with said predetermined label and said identity of a next peer for said information according to said path.

31

PATENT   Atty Docket No.: 100200290-1
                                               App. Ser. No.: 10/084,499

23. The method according to claim 22, further comprising:

    receiving a message, wherein said message comprises:

        said encryption key encrypted with a public key of said requestor;

        said information encrypted with said encryption key; and

        a message label; and

    retrieving said identity of next peer from said table in response to said message
label matching said predetermined label in said table.

24. The method according to claim 23, further comprising:

    encrypting said label with a public key of said next peer;

    reformatting said message with said label encrypted with said public key of said
next peer as said label; and

    transmitting said message to said next peer.

25. The method according to claim 23, further comprising:

    comparing said identity of said next peer with a current peer;

    decrypting said encryption key encrypted with a public key of said requestor in
response to said identity of said next peer being said current peer; and

    decrypting said information encrypted with said encryption key.

32

Atty Docket No.: 100200290-1
                                                                App. Ser. No.: 10/084,499

   26. (Canceled).

   27. The method according to claim 21, further comprising:

      forming a retrieval message comprising:

         said encryption key encrypted with said public key of said requestor;

         said encryption key encrypted with said public key of said provider;

         said transaction identifier, said reference for said information, and said

first next peer according to said path encrypted with said encryption key; and

      transmitting said retrieval message to said provider.

   28. The method according to claim 27, further comprising:

      applying a complementary key of said provider to said encryption key encrypted

with said public key of said provider; and

      decrypting said reference for said information, said transaction identifier, and said

first next peer.

   29. The method according to claim 28, further comprising:

      retrieving said information based on said reference for said information;

      encrypting said information with said encryption key; and

      forming a message label based on said transaction identifier.

PATENT   Atty Docket No.: 100200290-1
                                                 App. Scr. No.: 10/084,499

30. The method according to claim 29, further comprising:

   forming a message including said encrypted information and said message label;
and

   transmitting said message to said first next peer.

31-41. (Canceled).

42. A method of increasing peer privacy, comprising:

   forming a path for information from a provider to a requestor through a plurality

of peers in response to a received request for said information;

   transmitting to each peer of said plurality of peers a respective set-up message

comprising of a predetermined label and an identity of a next peer for said information;

   if a label stored at an intermediate peer of the plurality of peers does not match the

predetermined label in the set-up message, the intermediate peer stores the predetermined label

and the corresponding identity of the next peer;

   if a label stored at the intermediate peer matches the predetermined label, the

intermediate peer retrieves a previously stored message and generates a next state of the

predetermined label for the setup message; and

   transferring said information over said path in a message by determining a next

peer according to said path by matching a message label included in said message to said

predetermined label.

34

PATENT

43. The method of claim 42, wherein generating a next state further comprises:

encrypting the received predetermined label with a public key of a respective

index peer of the next peer.

44. The method of claim 42, wherein the stored message comprises:

an encryption key encrypted with the public key of the requestor.

35

PATENT   Atty Docket No.: 100200290-1
                                            App. Ser. No.: 10/084,499

(10)   Evidence Appendix

None.

36

PATENT

(11)   Related Proceedings Appendix

None.

37